ISO/IEC 15504-10 Safety Extension, Yet Another Safety Standard ?

Giuseppe Lami, PhD

Consiglio Nazionale delle Ricerche
Istituto di Scienza e Tecnologie dell'Informazione
via Moruzzi, 1 - Pisa

8° Workshop di
Automotive SPIN Italia

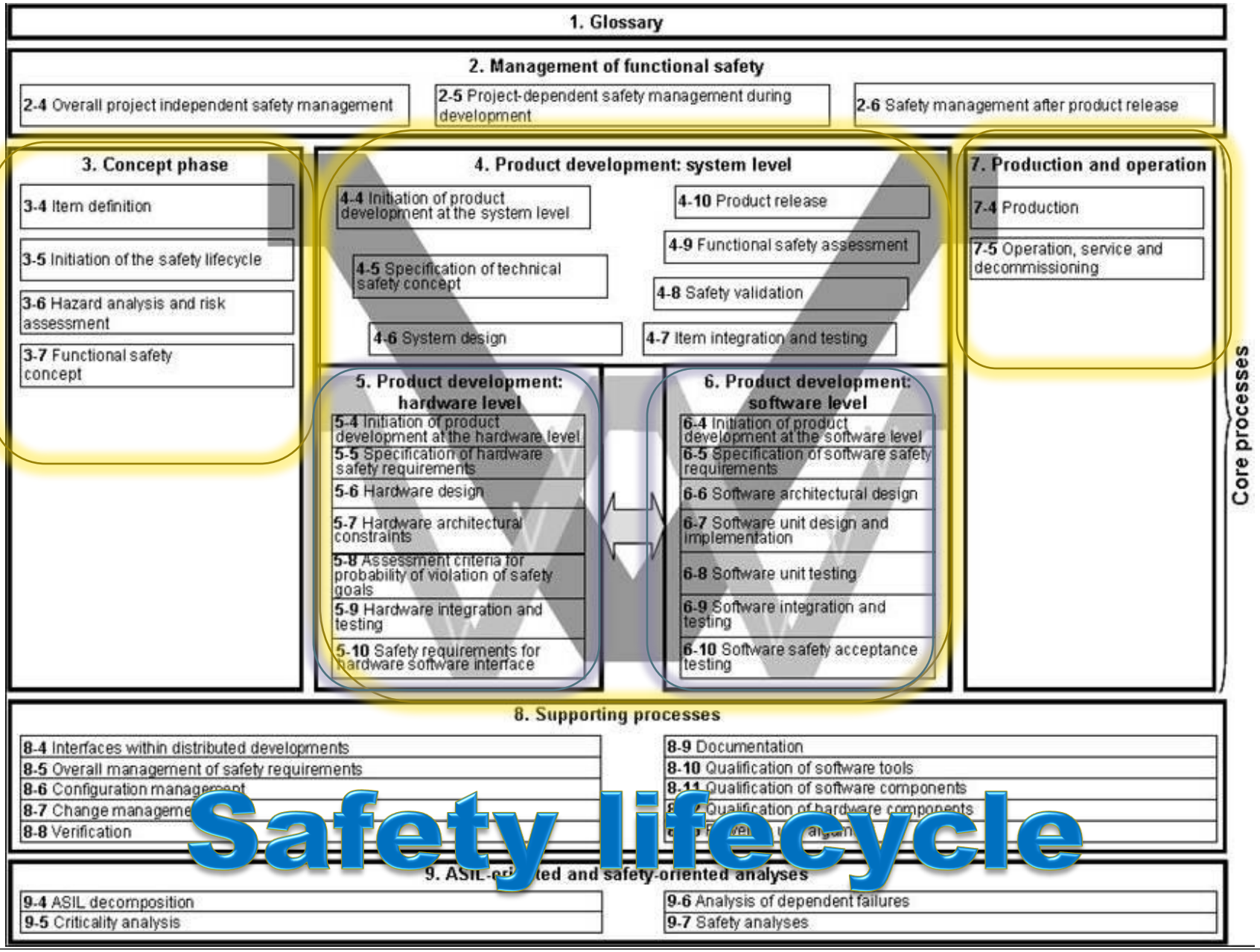
AUTOMOTIVE SPIN ITALIA

Milano, 17 Febbraio 2011

Talk outline

- Relationship between ISO 26262 & Automotive SPICE
- Overview of the last release of ISO/IEC 15504-10 Safety Extension (DTR ballot)
- How to integrate ISO 26262 & ISO/IEC 15504-10
- Conclusions

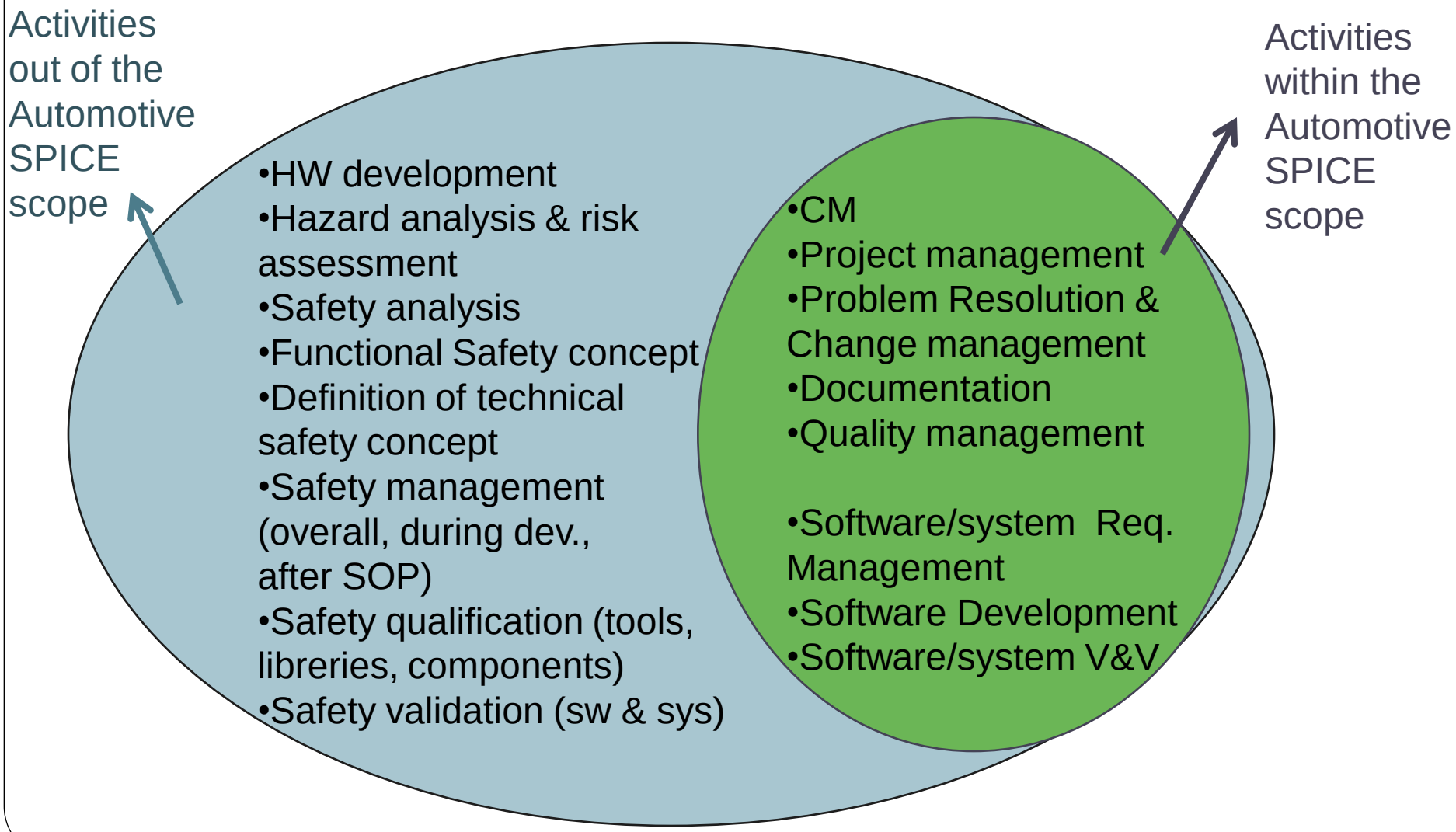
ISO 26262


1. Glossary
2. Management of functional safety
2-4 Overall project independent safety management
2-5 Project-dependent safety management during development
2-6 Safety management after product release
3. Concept phase
3-4 Item definition
3-5 Initiation of the safety lifecycle
3-6 Hazard analysis and risk assessment
3-7 Functional safety concept
4. Product development: system level
4-4 Initiation of product development at the system level
4-5 Specification of technical safety concept
4-6 System design
4-7 Item integration and testing
4-8 Safety validation
4-9 Functional safety assessment
4-10 Product release
5. Product development: hardware level
5-4 Initiation of product development at the hardware level
5-5 Specification of hardware safety requirements
5-6 Hardware design
5-7 Hardware architectural constraints
5-8 Assessment criteria for probability of violation of safety goals
5-9 Hardware integration and testing
5-10 Safety requirements for hardware software interface
6. Product development: software level
6-4 Initiation of product development at the software level
6-5 Specification of software safety requirements
6-6 Software architectural design
6-7 Software unit design and implementation
6-8 Software unit testing
6-9 Software integration and testing
6-10 Software safety acceptance testing
7. Production and operation
7-4 Production
7-5 Operation, service and decommissioning
Core processes
8. Supporting processes
8-4 Interfaces within distributed developments
8-5 Overall management of safety requirements
8-6 Configuration management
8-7 Change management
8-8 Verification
8-9 Documentation
8-10 Qualification of software tools
8-11 Qualification of software components
Qualification of hardware components
9. ASIL-oriented and safety-oriented analyses
9-4 ASIL decomposition
9-5 Criticality analysis
9-6 Analysis of dependent failures
9-7 Safety analyses
Safety lifecycle

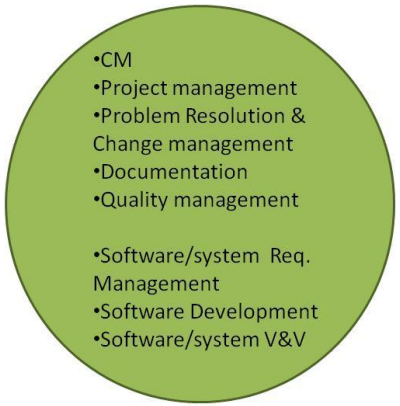
How does Automotive SPICE support the Safety Lifecycle?

- The support provided by Automotive SPICE to the ISO 26262 Safety Lifecycle is related to:
  - Project Management
  - CM
  - QM
  - ENG.*
  - Product release
  - Documentation
- From a producer point of view the goal is to understand the overlapping between.
  With a synergical perspective.

Overlapping between Automotive SPICE processes & ISO 262626 requirements



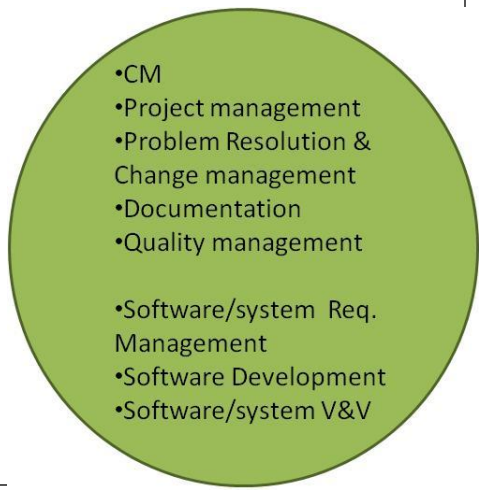
- It has been argued that having the Automotive SPICE processes (HIS scope, as a minimum) at level 2 provides support for the fulfillemnt of the ISO 26262 requirements
(see the *intersection area*).
[see E. Petry presentation @ 6W]



ISO 26262 ? Automotive SPICE

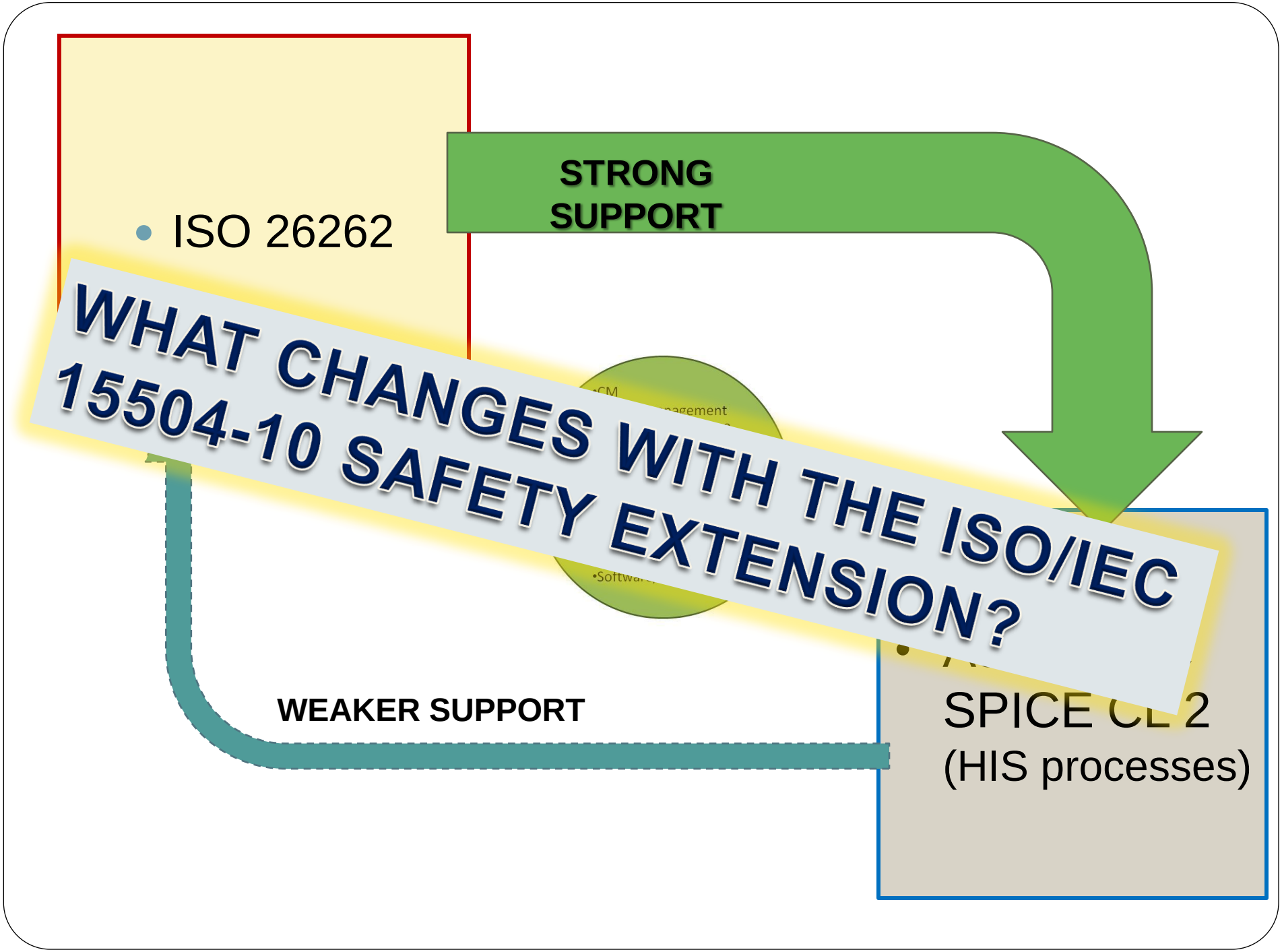
Scenario 1: ISO 26262 compliance

- Having achieved the ISO 26262 compliance for a certain project allow to infer the perfomance (and management) of processes (CM; PM; Problem resolution and change Man.; Documentation; QM; Requirements Man., Sw/System development, V&V) => achievement of Automotive SPICE capability level 1/2.
- It doesn't provides any guarantee of level 3 for processes



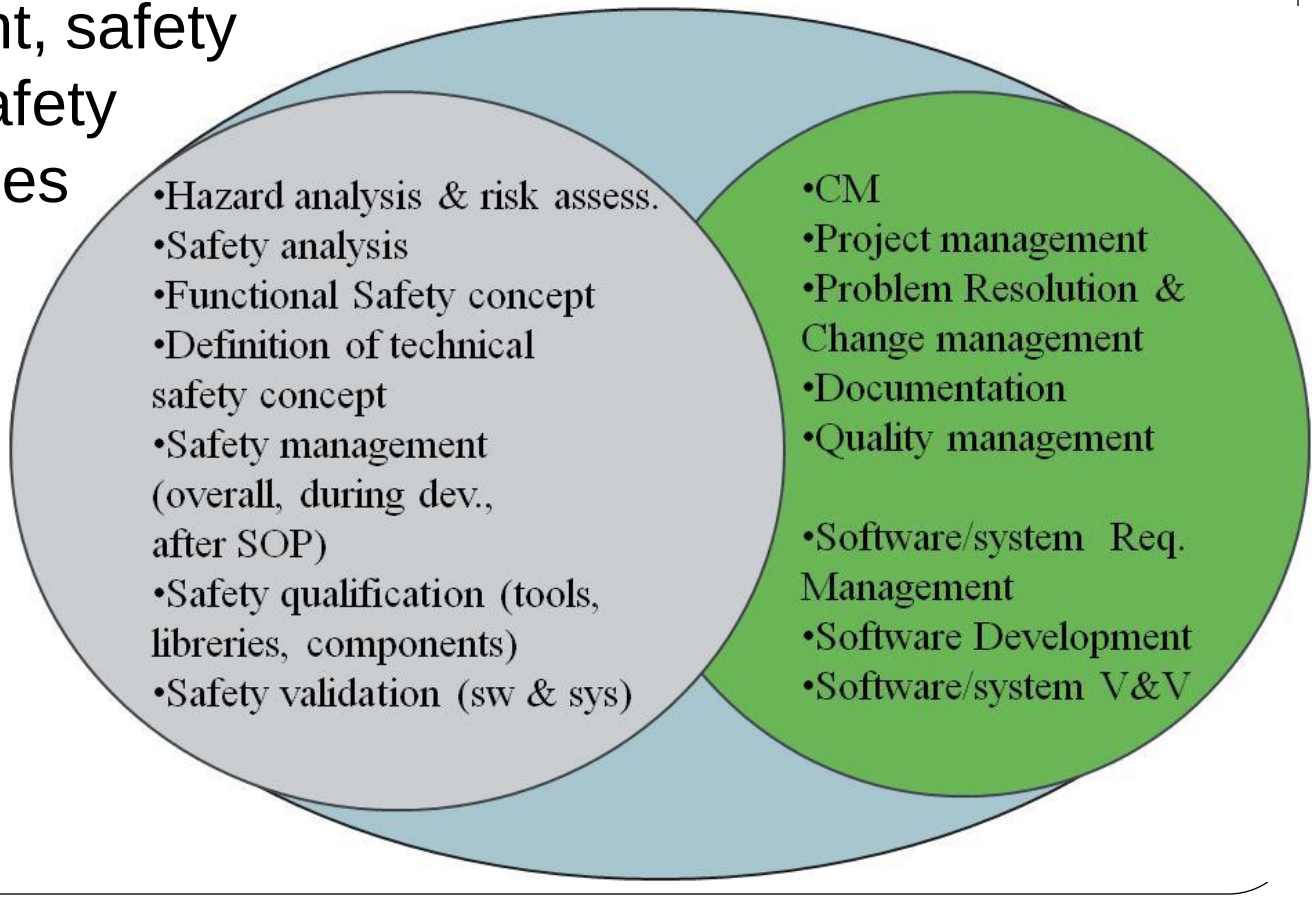
Scenario 2: Automotive SPICE (HIS processes) level 2

- It supports the achievement of compliance of ISO 26262 requirements for
  - CM; PM; Problem resolution and change Man.; Documentation; QM; Requirements Man.
  - Uncertain support for SW/Sys development and V&V. (because the ***way*** processes are performed may be different from the ***way*** required by the ISO 26262)
- It doesn't provide any guarantee for ISO 26262 compliance


ISO 26262
STRONG SUPPORT
WHAT CHANGES WITH THE ISO/IEC 15504-10 SAFETY EXTENSION?
WEAKER SUPPORT
SPICE CL 2
(HIS processes)

ISO 26262 vs. ISO/IEC 15504-10

- The goal of ISO 26262 (61508) is to demonstrate the capability to develop certain products with acceptable risks
- To do that the organization is required to perform defined safety management, safety engineering and safety qualification activities
- These activities correspond to the processes belonging to the ISO/IEC 15504-10 Safety Extension



ISO/IEC 15504-10 Safety Extension

Safety Management process (SAF.1): The purpose is to ensure that products, services and life cycle processes meet safety objectives

Process outcomes:

- Safety principles and safety criteria are established.
- The scope of the safety activities for the project is defined.
- Safety activities are planned and implemented.
- Tasks and resources necessary to complete the safety activities are sized and estimated.
- Safety organization structure (responsibilities, roles, reporting channels, interfaces with other projects or OUs …) is established.
- Safety activities are monitored, safety-related incidents are reported, analysed, and resolved.
- Agreement on safety policy and requirements for supplied products or services is achieved.
- Supplier's safety activities are monitored.

Base Practices:

- SAF.1.BP.1: Define safety objectives and criteria.
- SAF.1.BP.2: Define Safety Life Cycle.
- SAF.1.BP.3: Perform safety planning.
- SAF.1.BP.4: Define safety activities integration.
- SAF.1.BP.5: Define skills requirements definition and allocate responsibility.
  SAF.1.BP.6: Implement planned safety activities.
- SAF.1.BP.7: Monitor the deployment of the safety activities.
- SAF.1.BP.8: Define and agree safety policy and safety requirements with suppliers.
- SAF.1.BP.9: Monitor the safety activities of the supplier.
- SAF.1.BP.10: Implement an escalation mechanism.

ISO/IEC 15504-10 Safety Extension

Safety Engineering process (SAF.2): the purpose is to ensure that safety is adequately addressed throughout all stages of the engineering processes.

Process outcomes:

- Hazards related to product are identified and analysed.
- Hazard log is established and maintained.
- Safety demonstration for the product lifecycle is established and maintained.
- Safety requirements are defined.
- Safety integrity requirements are defined and allocated.
- Safety principles are applied to development processes.
- Impacts on safety of change requests are analysed.
- Product is validated against safety requirements.
- Independent evaluations are performed.

Base Practices:

- SAF.2.BP.1: Identify hazard sources and hazards.
- SAF.2.BP.2: Analyze hazards and risks.
- SAF.2.BP.3: Establish and maintain hazard log.
- SAF.2.BP.4: Establish and maintain safety demonstration.
- SAF.2.BP.5: Establish and maintain safety req.s.
- SAF.2.BP.6: Determine safety integrity requirements.
  NOTE : Safety integrity req. may be described i.e. as SIL.
- SAF.2.BP.7: Allocate safety requirements and safety integrity requirements.
- SAF.2.BP.8: Apply safety principles to achieve safety integrity requirements.
- SAF.2.BP.9: Perform safety impact analysis on changes.
- SAF.2.BP.10: Perform safety validations on product.
- SAF.2.BP.11: Perform independent assessments.

ISO/IEC 15504-10 Safety Extension

Safety Qualification process (SAF.3): the purpose is to assess the suitability of external resources when developing a safety-related software or system.

Process outcomes:

- Safety qualification strategy for external resources is developed.
- Safety qualification plan is developed and executed.
- Safety qualification documentation is written.
- Safety qualification report is produced.

Base Practices:

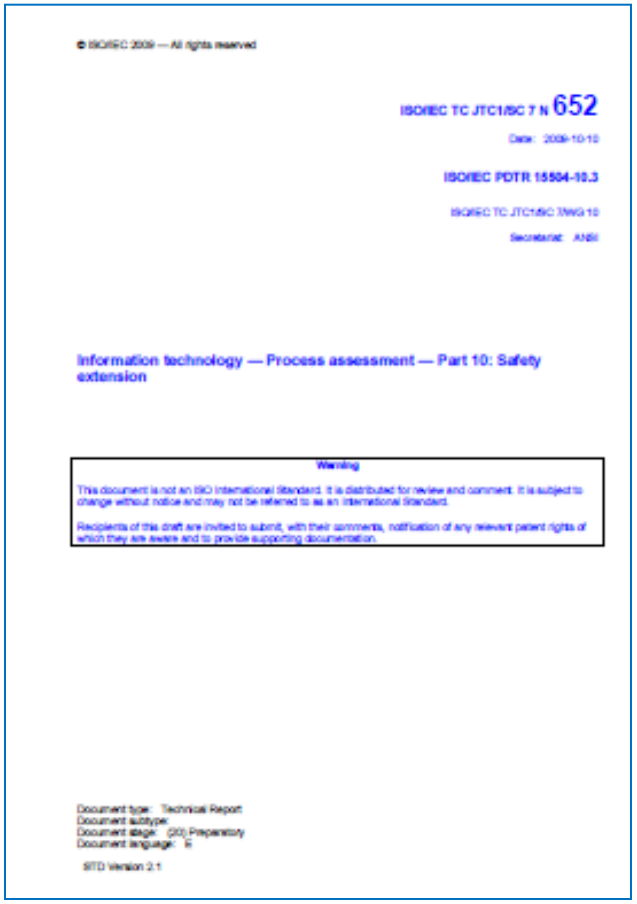
- SAF.3.BP.1: Develop a safety qualification strategy.
- SAF.3.BP.2: Plan the safety qualification of external resources.

  NOTE : Examples of external resources are as follows:
  - core engineering tools - automatic code generators, compilers and linkers;
  - engineering support tools - test, build and CM tools;
  - management support tools - documentation and project management tools.
- SAF.3.BP.3: Qualify the external resources.
- SAF.3.BP.4: Record the safety qualification results.
- SAF.3.BP.5: Maintain and update the safety qualification results.

ISO/IEC 15504-10
Realtionship among processes

ISO/IEC 15504-10 clause 5: Lifecycle Guidance

- It gives the assessors, for each process contained in 15504-5 and 15504-6, an indication of additional issues to be taken into account at assessment time.
- In Annex A WP characteristics are provided



ISO/IEC JTC1/SC 7 N 652

Date: 2009-10-10

ISO/IEC PDTR 15504-10.3

ISO/IEC JTC1/SC 7/WG 10

Secretariat: ANSI

Information technology — Process assessment — Part 10: Safety extension

Warning

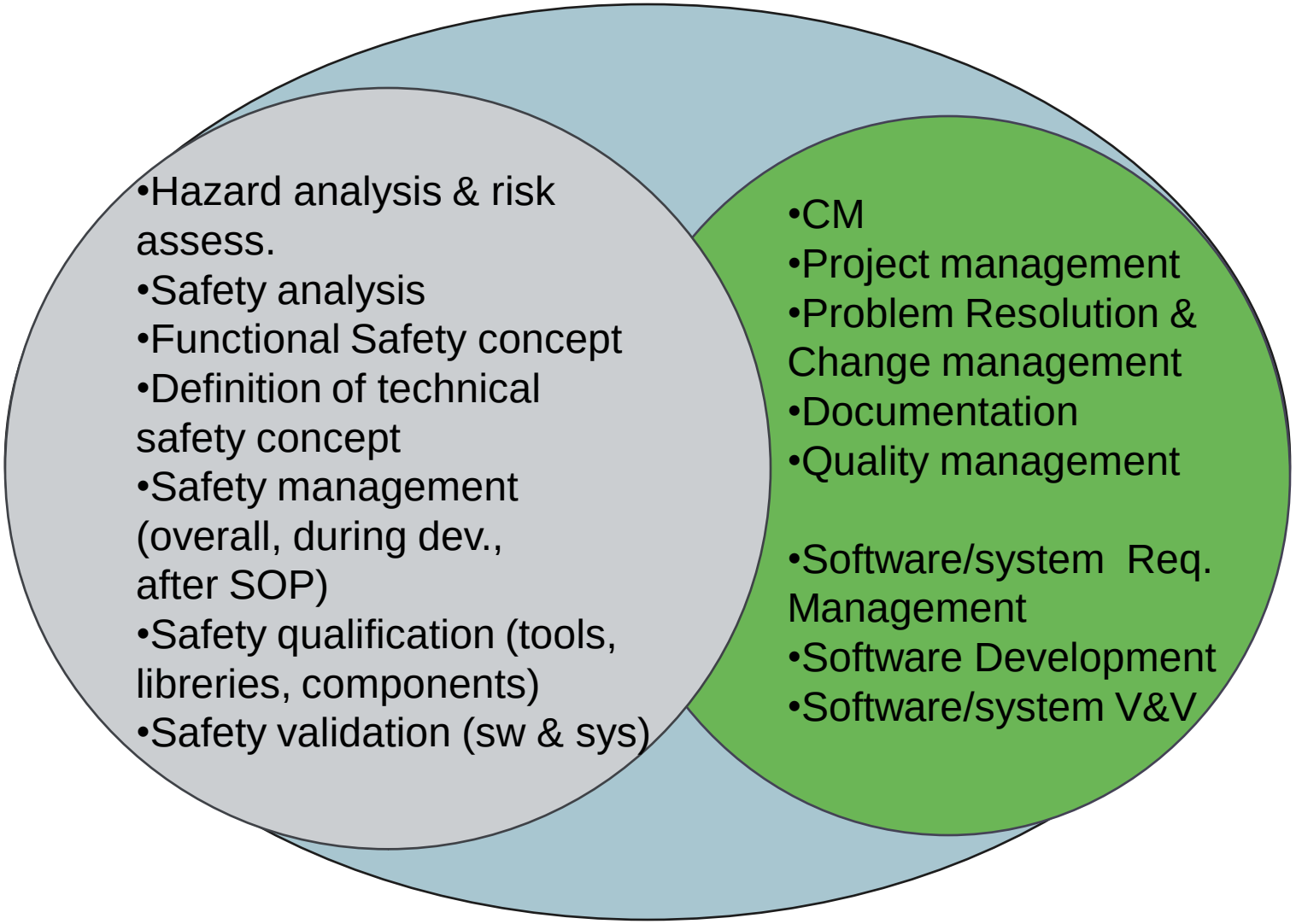
This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: Technical Report
Document subtype:
Document stage: (20) Preparatory
Document language: E

STD Version 2.1

ISO 26262 vs. ISO/IEC 15504-10



Realtionship between ISO 26262 & ISO/IEC 15504-10

Scenario 1: ISO 26262 compliance

- It is possible to infer the perfomance (and management) of processes into the HIS scope + those belonging to the ISO/IEC 15540-10 ⇨ achievement of Automotive SPICE (HIS) CL1/2 + CL 1/2 of the ISO/IEC 15504-10 processes.

Why should I spend effort for increasing the capability of ISO/IEC 15504-10 processes?

Scenario 2: Automotive SPICE (HIS)+ ISO/IEC 15504-10 (CL 2)

- It supports the achievement of compliance of ISO 26262 requirements for:
  - all the activties but
  - SW/Sys development and V&V. activities (because the ***way*** process are prerformed may be different from the ***way*** required by the ISO 26262)
- It doesn't provide any guarantee for ISO 26262 compliance

Why increasing ISO/IEC 15504-10 processes capability?

- Capability is not (only) performance
- Higher capability means:
  - Efficient and repeatable development
  - Lower risk of missing project objectives
  - Identification of improvement areas
- Improving the capability of 15504-10 processes:
  - Isn’t a short cut for ISO 26262 but
  - It is a way to improve safety-related processes
  - Is a managerial choice oreinted to process improvement
  - Is a way to extend the benefits of ten years of process improvement in automtive to safety-related activities

Thanks

- **Giuseppe Lami, PhD**

ISO/IEC 15504 & Automotive SPICE Principal Assessor

cert. N. Intacs-3961-1000-20254-03
cert. N. IntRSA 07/IntRSA-91004-I

Consiglio nazionale delle Ricerce
Istituto di Scienza e Tecnologia dell'Informazione (ISTI)
via Moruzzi,1 56124 Pisa (Italia)

phone: 0503153493
email: giuseppe.lami@isti.cnr.it